

005040 3534266

1 CLAIMS

2

3 1. A system supporting public key encryption, the system comprising:

4 a certifying authority;

5 a client device, coupled to the certifying authority, to,

6 generate a blinded certificate including a public key, and

7 transmit the blinded certificate to the certifying authority; and

8 wherein the certifying authority is to digitally sign the blinded certificate

9 and encode security attributes of the client device into the digital signature.

10

11 2. A system as recited in claim 1, wherein the client device is further to

12 receive the blinded certificate and generate a signed certificate by unblinding the

13 signed blinded certificate.

14

15 3. A system as recited in claim 1, further comprising a content server

16 coupled to provide electronic content to the client device

17

18 4. A system as recited in claim 3, wherein the client device is further to

19 generate a signed certificate by unblinding the signed blinded certificate and to

20 transfer the signed certificate to the content server, and wherein the content server

21 is to check security attributes of the client device based on attributes encoded into

22 the digital signature and to determine how to respond to the request based on the

23 security attributes.

24

25

5. A system as recited in claim 4, wherein the content server can respond by doing one or more of the following: determining whether to deliver the requested content, determining what quality of content to deliver, or determining what additional security precautions to require of the client device.

6. A system as recited in claim 1, wherein the certifying authority is to digitally sign the blinded certificate according to a formula

$$(\text{blinded certificate})^d \bmod (n),$$

wherein d represents a private key of the certifying authority and wherein n is a product of two prime numbers that comprise the private key.

7. A system as recited in claim 6, wherein the certifying authority is to encode a security attribute into the digital signature by:

representing the security attributes as a series of bits;

identifying, for each bit in the series that has a particular value, a corresponding integer; and

generating as the value d the product of the identified integers.

8. A system as recited in claim 7, wherein the certifying authority is further to generate another digital signature for the blinded certificate by:

additionally identifying, for each bit in the series that has another value, a corresponding integer; and

generating as the value d for the other digital signature the product of the additionally identified integers.

005040 9506450

1 9. A method comprising:
2 receiving, from a client, a current certificate and a request to sign a new
3 certificate;
4 determining attributes of the client based on the current certificate;
5 selecting, in accordance with public key cryptography, a public/private key
6 pair that is based at least in part on the attributes of the client; and
7 digitally signing the new certificate using the selected private key.

8
9 10. A method as recited in claim 9, wherein the attributes are security
10 attributes of the client.

11
12 11. A method as recited in 9, wherein the new certificate is a blinded
13 certificate.

14
15 12. A method as recited in 9, further comprising determining additional
16 information to encode into the digital signature, and wherein the selecting further
17 comprises selecting the public/private key pair based on the attributes of the client
18 and the additional information.

19
20 13. A method as recited in 9, wherein the selecting comprises
21 determining a bit pattern that corresponds to the security attributes of the client,
22 and identifying a public/private key pair that corresponds to the bit pattern.

0050403504260

1 **18.** An apparatus to digitally sign electronic information, the apparatus
2 comprising:

3 a connection module to establish a secure connection with a client device;
4 a signature module to receive electronic information from the client device
5 and digitally sign the electronic information, encoding attributes of the client
6 device into the digital signature.

7
8 **19.** An apparatus as recited in claim 18, wherein the attributes are
9 security attributes of the client device.

10
11 **20.** An apparatus as recited in claim 18, further comprising a certificate
12 archive that stores currently valid certificates issued by the apparatus, and wherein
13 the apparatus is further to receive a public key, check whether the certificate
14 archive stores a currently valid certificate corresponding to the public key, and
15 respond to the request based on the results of the checking.

16
17 **21.** A method comprising:
18 receiving, from a client, a request for electronic content;
19 checking, based on information encoded in a digital signature of at least a
20 portion of the request, whether the client has a set of claimed security attributes;
21 and
22 determining how to respond to the request based on the checking.

1 22. A method as recited in claim 21, wherein the determining how to
2 respond comprises one or more of: determining what quality level of content to
3 provide, determining what type of payment to require, and determining what
4 additional security precautions are required on the part of the client.

5
6 23. A method as recited in claim 21, wherein the checking comprises
7 determining a public key based on the set of claimed security attributes, and using
8 the public key to verify the digital signature.

9
10 24. A method as recited in claim 21, wherein the checking comprises:
11 representing the set of claimed security attributes as a series of bits;
12 generating a public key for a certifying authority using the series of bits;
13 and
14 using the public key to verify the digital signature.

15
16 25. A method as recited in claim 24, wherein the generating comprises:
17 identifying, for each bit in the series that has a particular value, a
18 corresponding integer; and
19 generating as the public key the product of the identified integers.

20
21 26. One or more computer-readable memories containing a computer
22 program that is executable by a processor to perform the method recited in claim
23 21.
24
25

1 27. A method comprising:
2 generating a public/private key pair for use in public key cryptography;
3 creating a certificate including the public key;
4 transmitting the certificate to a certificate archive; and
5 receiving, from the certificate archive, an indication of whether the
6 certificate is currently valid.

7
8 28. One or more computer-readable memories containing a computer
9 program that is executable by a processor to perform the method recited in claim
10 28.

11
12 29. A method for recovering from a device failure in a public key
13 encryption system, the method comprising the following acts:

- 14 (a) generating a public/private key pair using a fixed algorithm and a
15 fixed seed value;
16 (b) creating a certificate incorporating the public key;
17 (c) querying a certificate archive as to whether the certificate is valid;
18 (d) if the certificate is not valid, then generating a new public/private
19 key pair using the fixed algorithm and based on the public key;
20 (e) repeating acts (b) – (d) until a valid certificate is created.

21
22 30. One or more computer-readable memories containing a computer
23 program that is executable by a processor to perform the method recited in claim
24 29.
25